UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/779,440	02/09/2001	Kentaro Shiomi	60188-031	6677

7590 11/28/2005

MCDERMOTT WILL & EMERY
600 13TH STREET, N.W.
WASHINGTON, DC 20005-3096

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 11/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/779,440	SHIOMI ET AL.	
	Examiner	Art Unit	
	Jung W. Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,24 and 25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *2-7* is/are allowed.

6)☒ Claim(s) *1,24 and 25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the RCE filed on October 11, 2005.

2. Claims 1-7, 24 and 25 are pending.

3. Claims 8-23 are canceled.

4. Claims 24 and 25 are new.

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Continued Examination Under 37 CFR 1.114

6. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 11, 2005 has been entered.

Response to Arguments

7. Applicant's arguments on pg. 6, with respect to claim 1 have been fully considered but are not persuasive. Specifically, Applicant's argue that the prior art does not teach the step of "generating key data ..." since the predicates disclosed in the Collberg reference to obfuscate code are "previously inserted into the code as a

disguise and do not form key data (i.e. password) that would be inputted to obtain the correct code. Indeed, Collberg simply integrates correct and dummy code using the predicates, thereby hiding the correct code from reverse engineers ... Collberg is unrelated to key data used to operate the correct code."

8. In determining the relevancy of Collberg with the claimed invention the limitation, key data, was given its broadest meaning (MPEP 2111). It is noted that in view of Applicant's specification, there does not appear to be a special meaning associated with the term, rather, it appears that "key data" is given a wide scope to include such values as selection signals (see claim 2). Since claim 1 does not further limit "key data" except that the encrypted circuit data does not operate as targeted without input of such "key data," it was determined that the selection mechanism of Collberg was within the scope of "key data", since the predicate of Collberg operates as a selection signal between two flow paths, one of which is the original flow path and the other is a dummy flow path; without this predicate being a "true" value, the program would not function as targeted. Also the fact that the predicate is "previously inserted" into the code does not preclude it from covering the claimed limitation of "inputting the key data" since there is no condition in the claims of when the key data is to be inserted into the encrypted circuit; it presumed that the key data is inserted anytime prior to operating the LSI for proper operation. Furthermore, the fact that the particular example of the key data of Collberg always selects the correct version of the code is evidence of the fact that the key data is a *selection signal* that enables proper operation of the obfuscated program as recited in the limitation of claim 1.

9. Finally, in reply to Applicant's allegation that Collberg does not provide motivation to combine the obfuscation of software-based code with the obfuscation of hardware programs, the Examiner respectfully disagrees. As indicated in the previous action, Collberg teaches obfuscation using "key data" and reasons why this is desirable. In addition, Johnson '741 identifies similarities between hardware and high level software encoding properties to generate encoded programs (col. 7:66-8:48). Hence, enhancements in software obfuscation techniques have corresponding enhancements in hardware obfuscation techniques.

10. For these reasons, claim 1 remains rejected under Johnson in view of Collberg.

Claim Rejections - 35 USC § 112

11. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

12. Claims 1 and 25 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The claims recite the limitation "wherein the encrypted circuit design data does not operate as targeted without inputting the key data into the LSI." However, there is no basis in the original disclosure to support the negative limitation "does not operate as targeted without inputting the key data into the

LSI." (see MPEP 2173.05(i)). Nowhere in the specification does it disclose improper operation of the program when the key data is not inputted into the LSI. As best ascertained from the disclosure, the key data is a selection signal for selecting a number of signals corresponding to the number of outputs of an original circuit from an output from a permutation circuit so as to produce encrypted circuit design data, and wherein such a value of the key signal that the output of the original circuit matches an output of the selector is used as a key of the encrypted circuit data (Specification, figs. 4, 5C-D and claim 2).

13. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

14. Claims 1, 24 and 25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

15. Claims 1, 24 and 25 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. The omitted structural cooperative relationships are: generating or providing permutation circuit design data for permutating respective outputs of the original circuit design data with the dummy circuit design data (without such a cooperative relationship, the converting step is not possible; see Specification, fig. 4, reference no. 21).

16. Claims 1, 24 and 25 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01. The omitted elements are: the key data being a selection signal for selecting a number of signals corresponding to the number of outputs of an original circuit from an output from a permutation circuit so as to produce encrypted circuit design data, and wherein such a value of the key signal that the output of the original circuit matches an output of the selector is used as a key of the encrypted circuit data (this is an essential feature of the key data: the specification only enables the invention where the key data is a selector signal to select from outputs from a permutation circuit, and without this property, the claims do not sufficiently identify the essential interrelationship between the step of converting the circuit design and the step of generating key data; see Specification, figs. 4 and 5C-D).

Claim Rejections - 35 USC § 103

17. Claims 1, 24 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson et al. USPN 6,088,452 (hereinafter Johnson) in view of Collberg et al. "Manufacturing Cheap, Resilient, and Stealthy Opaque Constructs" (hereinafter Collberg).

18. As per claim 1, Johnson discloses a method for designing a circuit, comprising the step of encrypting provided circuit design data (Johnson, Abstract), the encrypting step includes the steps of:

a. generating dummy circuit design data; converting the circuit design data into encrypted circuit design data by combining the circuit design data and the dummy circuit design data (Johnson, col. 12:9-20).

19. Johnson does not expressly disclose generating key data, wherein the encrypted circuit design data does not operate as targeted without inputting the key data into the circuit. Collberg discloses multiple opaque constructs wherein irrelevant code is inserted into an original code by means of a branch insertion transformation (Collberg, fig. 4(c)); an opaque predicate is set to a value (true) so that the branch operation correctly directs the operation of the program to the correct version of the code. This value is the key data of the obfuscation technique disclosed by Collberg. Moreover, although Collberg discloses such limitations in the context of software design rather than hardware design, the two areas are closely linked: Johnson discloses that hardware design and high-level programming languages are generally be encoded based on similar principles (Johnson, col. 7:67-8:48). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the encryption step of Johnson to generate key data, wherein the encrypted circuit design data does not operate as targeted without inputting the key data into the LSI, since the insertion of dummy data by a branch insertion transformation instills more complexity and hence better obfuscation of program design. Collberg, section 4.2, 1st paragraph. The aforementioned cover the limitations of claim 1.

20. As per claim 24, Johnson discloses a method for designing a circuit, comprising the step of encrypting provided circuit design data (Johnson, Abstract), the encrypting step includes the steps of:

b. generating dummy circuit design data; converting the circuit design data into encrypted circuit design data by combining the circuit design data and the dummy circuit design data (Johnson, col. 12:9-20).

21. Johnson does not expressly disclose generating real key data and dummy key data, wherein the circuit design data is selected to operate as targeted with the real key data and the dummy circuit design data is selected to operate with the dummy key data. Collberg discloses multiple opaque constructs wherein irrelevant code is inserted into an original code by making the termination condition more complex (Collberg, fig. 5(d)). In this example, the original predicate is a variable i having an initial value; another predicate is added to the condition such that the predicate is evaluated to true regardless of the assignment of a new variable j. This disclosure of Collberg suggests that the feature of providing real key data and dummy key data are obvious implementations in the field of obfuscation of program design. Moreover, although Collberg discloses such limitations in the context of software design rather than hardware design, the two areas are closely linked: Johnson discloses that hardware design and high-level programming languages are generally be encoded based on similar principles (Johnson, col. 7:67-8:48). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the encryption step of Johnson to generate a real key data and dummy key data, wherein the circuit design

data is selected to operate as targeted with the real key data and the dummy circuit design data is selected to operate with the dummy key data, since conditional transformations that insert additional predicates within a program instills more complexity and hence better obfuscation of program design. Collberg, section 4.3, 1st paragraph. The aforementioned cover the limitations of claim 24.

22. As per claim 25, Johnson discloses a method for designing a circuit, comprising the step of encrypting provided circuit design data (Johnson, Abstract), the encrypting step includes the steps of:

c. generating dummy circuit design data having a same number of inputs and a same number of outputs as those of the circuit design data; converting the circuit design data into encrypted circuit design data by combining the circuit design data and the dummy circuit design data (Johnson, col. 12:9-20, especially, lines 20-21).

23. Johnson does not expressly disclose generating key data, wherein the encrypted circuit design data does not operate as targeted without inputting the key data into the circuit. Collberg discloses multiple opaque constructs wherein irrelevant code is inserted into an original code by means of a branch insertion transformation (Collberg, fig. 4(c)); an opaque predicate is set to a value (true) so that the branch operation correctly directs the operation of the program to the correct version of the code. This value is the key data of the obfuscation technique disclosed by Collberg. Moreover, although Collberg discloses such limitations in the context of software design rather

than hardware design, the two areas are closely linked: Johnson discloses that hardware design and high-level programming languages are generally be encoded based on similar principles (Johnson, col. 7:67-8:48). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the encryption step of Johnson to generate key data, wherein the encrypted circuit design data does not operate as targeted without inputting the key data into the LSI, since the insertion of dummy data by a branch insertion transformation instills more complexity and hence better obfuscation of program design. Collberg, section 4.2, 1st paragraph. The aforementioned cover the limitations of claim 25.

Allowable Subject Matter

24. Claims 2-7 are allowed.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

November 17, 2005

GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100